IN THE UNITED STATES COURT OF APPEALS
FOR THE FIFTH CIRCUIT

United States Court of Appeals
Fifth Circuit

FILED

December 16, 2008

Charles R. Fulbruge III
Clerk

No. 08-40169

UNITED STATES OF AMERICA

Plaintiff-Appellee

v.

JOHN CRAIG ZIMMERMAN

Defendant-Appellant

Appeal from the United States District Court
for the Southern District of Texas
No. 1:07-CR-232-1

Before SMITH, BARKSDALE, and PRADO, Circuit Judges.

PER CURIAM:[*]

Having conditionally pleaded guilty, John Craig Zimmerman challenges his convictions for: sexual exploitation of a child for the purpose of producing child pornography, in violation of 18 U.S.C. §§ 2251(a) and 2; receipt of child pornography, in violation of 18 U.S.C. §§ 2252A(a)(2)(B), 2256(8), and 2; and possession of child pornography, in violation of 18 U.S.C. §§ 2252A(a)(4)(B), 2252(b)(2), and 2. At issue is whether the district court erred in denying

[*] Pursuant to 5TH CIR. R. 47.5, the court has determined that this opinion should not be published and is not precedent except under the limited circumstances set forth in 5TH CIR. R. 47.5.4.

Zimmerman's motion to suppress evidence obtained from his City-owned workplace computer and his residence. AFFIRMED.

I.

On 5 February 2007, the Brownsville Fire Department (BFD) received an anonymous tip that Zimmerman, one of its employees, had pornographic photographs of children on his City-owned workplace computer. Previously, in 2003, Zimmerman had been under investigation for similar suspicions involving child pornography. On that occasion, upon searching his workplace computer, officials found no evidence of such pornography.

On the evening of 6 February 2007, an employee of the MIS department–the entity responsible for managing all major computer issues for the City–searched Zimmerman's workplace computer, without a warrant, and discovered adult pornography, as well as encrypted information. The MIS employee decoded the information and uncovered many pornographic images, some of which he suspected to be child pornography. That same evening, the BFD fire chief informed the Brownsville Police Department (BPD) that what was believed to be child pornography had been found on a City computer.

After showing the images to a BPD detective and an Immigrations and Customs Enforcement (ICE) Agent, the MIS employee signed a written consent form authorizing the BPD to take possession of Zimmerman's workplace computer. Agents then obtained a search warrant for Zimmerman's home. Claimed probable cause was founded on the images obtained from his workplace computer, as well as an affidavit by an ICE Special Agent stating: based on her training and experience, because child pornography had been found on Zimmerman's workplace computer, he would have it at his home as well.

On 9 February 2007, Zimmerman's residence was searched and approximately 1200 images and 17 videos of child pornography were seized. Two

females later testified that Zimmerman had taken photos of them, with and without clothes, several years earlier when they were underage.

In April 2007, Zimmerman was indicted on four counts of violating the Child Pornography Prevention Act, 18 U.S.C. § 2252A. He pleaded not guilty and moved to suppress the evidence he claimed was illegally seized: the images on the workplace computer and those found at his residence.

The district court held an evidentiary hearing on 6 August 2007 and subsequently, through a comprehensive opinion, denied the motion, determining: Zimmerman did not have a reasonable expectation of privacy in his workplace computer; assuming, arguendo, Zimmerman had such an expectation, the initial search of the workplace computer did not violate his Fourth Amendment rights, because BFD officials had an objectively justifiable suspicion to initiate a reasonable search; the MIS employee had authority to consent later to the search of the workplace computer by law enforcement; and, the search warrant for Zimmerman's home properly flowed from the evidence obtained from the workplace computer and the ICE Special Agent's affidavit. United States v. Zimmerman, No. B-07-232 (S.D. Tex. 22 Aug. 2007) (District Court's Order denying motion to suppress).

Reserving the right to appeal the denial of his suppression motion, Zimmerman pleaded no contest to three of the four counts in the indictment. (The district court granted the Government's motion to dismiss the other count.) On 8 February 2008, the district court sentenced Zimmerman, inter alia, to 300 months' imprisonment.

II.

For reviewing the denial of a suppression motion, the district court's conclusions of law are reviewed de novo; its factual findings, only for clear error. E.g., United States v. Lopez-Moreno, 420 F.3d 420, 429 (5th Cir. 2005). In reviewing findings of fact, the evidence is viewed in the light most favorable to

the prevailing party on the motion (here, the Government). Id. Essentially for the reasons stated in the district court's opinion, the suppression motion was properly denied.

A.

Zimmerman first contends the search of his City-owned workplace computer violated his Fourth Amendment rights. That Amendment guarantees "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures". U.S. CONST. amend. IV. The touchstone of Fourth Amendment analysis is whether the defendant had a constitutionally protected reasonable expectation of privacy in the item searched and seized by the Government. California v. Ciraolo, 476 U.S. 207, 211 (1986); United States v. Slanina, 283 F.3d 670, 675 (5th Cir. 2002).

The district court's findings of fact are not clearly erroneous. Viewing the evidence in the requisite light most favorable to the Government, we conclude Zimmerman did not have an objectively reasonable expectation of privacy in his City-owned workplace computer. Of course, as application of the Fourth Amendment hinges on finding an expectation of privacy, there can be no constitutional violation without one. Smith v. Maryland, 442 U.S. 735, 740 (1979). Thus, the procedure employed for Zimmerman's workplace computer by City officials did not constitute a "search" for Fourth Amendment purposes.

Additionally, it was not clear error for the district court to determine the MIS employee gave voluntary consent, as a third party possessing authority and common control over the item to be searched, to the BPD Agents to seize the workplace computer, justifying the warrantless search. See United States v. Matlock, 415 U.S. 164, 171 (1974). As such, the motion to suppress evidence found on Zimmerman's workplace computer was properly denied.

B.

Zimmerman also contends the evidence obtained from the search of his residence was inadmissible because it was the "fruit" of the claimed illegal search of his workplace computer and therefore tainted by that prior procedure. See Wong Sun v. United States, 371 U.S. 471, 487-88 (1963). As held above, evidence obtained from that workplace computer was not "tainted". Nevertheless, a discussion follows for the proper procedure employed in this instance.

The district court concluded that the affidavit of the ICE Special Agent, supporting the issuance of the search warrant for Zimmerman's residence, supplied a "substantial basis for determining the existence of probable cause". Illinois v. Gates, 462 U.S. 213, 239 (1983). Additionally, it determined: using evidence from the workplace search in obtaining the search warrant did not violate Zimmerman's Fourth Amendment rights, because, as noted, that procedure was constitutionally reasonable. Giving the requisite deference to the district court's findings of fact, and in the light of our holding supra that the evidence obtained from Zimmerman's workplace computer was not "tainted", Zimmerman's motion to suppress evidence found in his home was properly denied.

III.

For the foregoing reasons, the judgment is AFFIRMED.